



REPLY TO  
ATTENTION OF

**DEPARTMENT OF THE ARMY**  
US ARMY INSTALLATION MANAGEMENT COMMAND  
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT BELVOIR  
9820 FLAGLER ROAD, SUITE 213  
FORT BELVOIR, VIRGINIA 22060-5928

IMNE-BEL-IMA

11 August 2008

MEMORANDUM FOR US Army Fort Belvoir Personnel

SUBJECT: Fort Belvoir Policy Memorandum #32, Information Assurance (IA) Program

1. REFERENCES:

- a. Public Law 100-235, The Computer Security Act of 1987.
- b. DODI 8510.01, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007.
- c. DODD 8500.1E, Information Assurance (IA), 24 October 2002, 23 April 2007.
- d. DODI 8500.2, Information Assurance (IA) Implementation, 6 February 2003.
- e. AR 25-2, Information Assurance, 24 October 2007 (effective 13 November 2007).
- f. Best Business Practice, 05-PR-M-0002, Information Assurance (IA) Training and Certification, 9 March 2007.

2. PURPOSE: To implement command policy of compliance with statutes, regulations, and policies governing the Information Systems Security/Information Assurance (ISS/IA) Program. This program requires our full attention to ensure all information is protected.

3. APPLICABILITY: This policy applies to all military, civilian, tenant and personnel activities that plan, deploy, configure, operate and maintain data communications resources directly or indirectly attached to the Fort Belvoir Campus Area Network (CAN). This policy memorandum supersedes Fort Belvoir Policy Memorandum #32, 1 August 2007.

4. RESPONSIBILITIES:

- a. The installation Information Assurance Manager (IAM) is responsible for implementing the ISS/IA Program. The Installation Garrison Commander is the designated approving authority for the CAN.

**“EXCELLENCE THROUGH SERVICE”**

IMNE-BEL-IMA

SUBJECT: Fort Belvoir Policy Memorandum #32, Information Assurance (IA) Program

b. Each organization will appoint an individual in their organization to serve as the Information Assurance Security Officer (IASO), System Administrator (SA), or Network Manager (NM), as appropriate, and to be responsible for implementing ISS/IA requirements and responding to the installation's IAM.

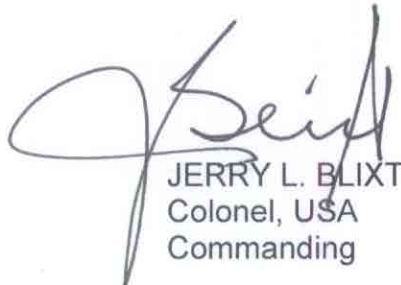
c. Individuals assigned the duties and responsibilities as IAM, IASO, SA, or NM will be trained in accordance with reference 1f, located at <https://informationassurance.us.army.mil/bbp/>.

d. Directorate of Information Management IA staff will conduct inspections to ensure provisions of paragraph 4b and 4c above are being implemented and in compliance with statutes, regulations and policies. Inspections will be coordinated with organization IASOs.

e. Support for the ISS/IA program is essential to protecting the CAN from illegal and damaging activity. To ensure continued confidentiality, integrity, and availability of information, our information technology assets must be protected.

5. POLICY: The Computer Security Act of 1987 requires the establishment of a computer security program for all "Federal" computer systems. The term "Federal" applies to all computer systems operated by a Federal agency or a contractor of a Federal agency or any organization/activity that processes information on behalf of the Federal Government. AR 25-2 establishes policy to implement IA requirements developed for responding to the IA challenge.

6. PROPONENT: The proponent and responsible agency of this policy is the Fort Belvoir Directorate of Information Management, Information Assurance Division, at 703-704-1582.



JERRY L. BLIXT  
Colonel, USA  
Commanding